Design and implementation of an integrated accounting architecture for distributed UMTS and WLAN networks

Racz, Peter ; Förster, Volker ; Stiller, Burkhard

Abstract: Accounting for resource and service usage in communication networks forms the basis of network operators' business, and is therefore essential. Within a heterogeneous, multidomain mobile environment of emerging new access technologies, the demand for a distributed accounting infrastructure becomes more relevant. Driven by the analysis of current accounting solutions in Universal Mobile Telecommunications System (UMTS) and Wireless Local Area Networks (WLAN) networks, the newly developed approach presents an integrated accounting architecture based on the Diameter protocol, forming a flexible basis for charging UMTS and WLAN communication services. The system developed is described, discussed and evaluated by a prototypical implementation.

DOI: https://doi.org/10.1504/IJWMC.2007.016721

A Design and Implementation of an Integrated Accounting Architecture for Distributed UMTS and WLAN Networks*

Peter Racz[1], Volker Förster, Burkhard Stiller[1,2]

[1] Communication Systems Research Group, Department of Informatics (IFI), University of Zurich, Switzerland
Winterthurerstrasse 190, CH—8057 Zurich, Switzerland
[2] Computer Engineering and Networks Laboratory (TIK), ETH Zurich, Switzerland
Gloriastrasse 35, CH—8057 Zurich, Switzerland

E-Mail: racz@ifi.uzh.ch, VolkerFoerster@bundeswehr.org, stiller@ifi.uzh.ch

Abstract

Accounting for resource and service usage in communication networks forms the basis of network operators' business, and is therefore essential. Within a heterogeneous, multi-domain mobile environment of emerging new access technologies, the demand for a distributed accounting infrastructure becomes more relevant. Driven by the analysis of current accounting solutions in UMTS and WLAN networks, the newly developed approach presents an integrated accounting architecture based on the Diameter protocol, forming a flexible basis for charging UMTS and WLAN communication services. The system developed is described, discussed, and evaluated by a prototypical implementation.

Keywords: *Distributed Accounting, Charging, Multi-domain Environments, Diameter, UMTS, WLAN.*

1 Introduction

Traditional network usage was driven by a number of different applications and customer requirements. Besides the fixed networking infrastructure and customers being located at well-defined locations within this domain, the upcoming wireless access network technologies have changed network management support functionality for customers. In addition, wireless environments are dominated by a quite high rate of customer mobility [3], [17], which needs to cross different technologies, and which requires the support of roaming between those environments. Different technologies have their own accounting mechanisms, which do not allow for an interoperability in most cases [20], [24]. But network providers need an integrated accounting architecture that enables to apply a common accounting process for different technologies in order to reduce configuration and management efforts and costs. Additionally, hotspots based on Wireless Local Area Networks (WLAN) and cellular networks, such as UMTS (Universal Mobile Telecommunications System) are often operated by different providers. Interoperability between them is inevitable for granting users access to the Internet being at varying locations and using different technologies. With the use of WLAN hotspots for example the user, who is confronted with different providers, is not willing to disconnect his device when leaving the network of one provider and to connect again, when entering the network of another. While each individual technology does not show this problem — a GSM (Global System for Mobile Communications) network of a single provider usually covers the entire area of a country — in tomorrow's scenario, where high capacity hotspots are available, the user wants to choose different offers in order to achieve the highest bandwidth available, even though this implies the use of a hotspot, whose operator is not the user's GSM provider.

The key success factor of this scenario is dominated by a successful interoperability between providers in terms of accounting and in support of charging [5], [24]. Initially, forcing a user to sign up with every provider confronted with is not an acceptable solution, since it does restrict the mobility of a user due to administrative boundaries. Therefore, a distributed accounting approach is of utmost importance, which enables multiple providers to collect information on users' activities. The overall goal of distributed accounting is to allow the transmission of accounting data between networks that do not operate on similar technology and do not belong to a single administration. A provider has to be able to use accounting information of users, who are not his own subscribers, for network management, traffic control, or access control. Fundamental requirements derived from a distributed accounting system result in a system, which has to be maintained easily, which needs to be scalable with respect to the number of users involved, and is required to be adaptable to different provider needs.

In commercial network environments user authentication, access control, and accounting of resource and service usage are essential from the provider's point of view. An AAA infrastructure (Authentication, Authorization and Accounting) [19] including related AAA protocols [12], [25] supports many functions, but distributed accounting schemes are more difficult. Accounting data of mobile users has to be forwarded to the home provider and his accounting server, and accounting data collected needs to be adapted in support of several different network technologies. Furthermore, network providers, where the user is currently attached to, need to keep track of users' activities. This work developed in due course addresses those requirements and outlines a detailed design and a prototypical implementation of an integrated accounting architecture for distributed multi-technology networks.

The remainder of this paper is structured as follows. While Section 2 summarizes related work in accounting in general, Section 3 outlines key technical details of the background network technology applied, such as accounting and charging in

* This work was performed, while all authors have been with the Information Systems Laboratory IIS at the University of Federal Armed Forces Munich, Germany.

UMTS and WLAN. The multi-domain, multi-technology scenario in Section 4 forms the basis for the detailed design of the distributed approach of Section 5. The prototypical implementation is discussed and evaluated in Section 6, before final conclusions are drawn in Section 7.

2 Related Work

The Internet Engineering Task Force (IETF) worked on AAA issues, in which the accounting part is of relevance for related work. The generic AAA architecture [19] defines common network components and AAA functionality together with a layered AAA protocol structure. It was designed to support different underlying technologies as well as multi-domain environments. Extending the generic architecture, a framework to provide authorization in a standard AAA environment is specified in [27]. It also defines possible trust relationships between client and server, and among servers for intra- and inter-domain environments. [7] discusses the purposes of accounting like billing, capacity planning and trend analysis. It also defines different data collection models between client and server together with requirements for the accounting process focusing on reliability, fault resilience, and failover mechanisms. Different accounting record formats are summarized in [9]. Policy-based accounting [28] extends the generic architecture with a policy-based configuration management considering both intra- and inter-domain accounting.

RADIUS (Remote Authentication Dial In User Service) [26], the most widely deployed AAA protocol in current network environments, was initially designed to support AAA functions in dial-up and terminal server access services. Accounting support in RADIUS was specified later on in [25]. With the increasing population of mobile users and the emerging new access technologies like WLAN the provision of AAA mechanisms is getting more difficult, and security aspects also become more relevant. As RADIUS is not able to meet all of the emerging requirements completely, IETF developed a new AAA protocol, Diameter, which is expected to replace RADIUS.

The Diameter protocol is divided into two parts, the Diameter base protocol [12] and Diameter applications. The base protocol provides basic services necessary for applications, which include delivering Diameter messages, negotiating capabilities between Diameter nodes, and error handling. Diameter applications, on the other hand, specify service-specific extensions and data units. There are several applications currently under development like the network access server (NAS) [13] and the mobile IPv4 [11] applications. The first one defines extensions required for the provisioning of a network access service, and specifies basic accounting attributes like session duration and transferred data volume. The latter one deals with AAA functionality in a multi-domain, mobile IPv4 environment, integrating home agent (HA) and foreign agent (FA) into the AAA architecture. It also considers how to correlate accounting information across hand-overs.

Opposite to the strict client-server model of RADIUS, Diameter is a peer-to-peer protocol in the sense, that any Diameter node can initiate a request. The protocol defines three different kinds of Diameter nodes. These are the clients, servers and agents. Clients are in general NAS devices controlling network access or other network components providing diverse services for end-users. Servers receive AAA requests from clients, and are responsible for AAA decisions in a particular domain. Agents provide either relay, proxy, redirect, or translation services. Similar to RADIUS, Diameter messages and data units are coded in AVPs (Attribute-Value-Pair), which allow the protocol to be extended in a flexible manner. Diameter runs over the TCP (Transmission Control Protocol) or SCTP (Stream Control Transmission Protocol) transport protocols, both providing a reliable transport mechanism. Additionally, Diameter supports secure communication based on IPSec (Internet Protocol Security) and TLS (Transport Layer Security) in intra- and inter-domain scenarios. Finally, it has a peer discovery and capability exchange mechanism, and it supports failover algorithms and a better error handling.

TACACS+ (Terminal Access Controller Access Control System) is an AAA protocol developed by Cisco Systems. It supports reliable transport of AAA messages over TCP, which makes it resistant against packet loss. The protocol offers start, stop, and interim messages for accounting purposes. Hop-by-hop authentication, integrity protection as well as hop-by-hop confidentiality is supported by TACACS+ [7].

Other protocols capable to transfer accounting information are the Simple Network Management Protocol (SNMP) and the Common Open Policy Service (COPS) protocol. SNMP is widely deployed in intra-domain management applications, and it can be used to collect accounting data typically by polling network equipment in regular intervals. It supports the transfer of accounting records in SNMP management information base (MIB), but it cannot be considered as a general AAA protocol [20]. COPS [16] was originally designed for the exchange of policy information between a policy decision point (PDP) and policy enforcement points (PEP). The communication is based on a query-response sequence. It supports reliable transport based on TCP, and it can be used to transfer accounting related messages. COPS is considered acceptable as an AAA protocol [20].

The EU IST project MobyDick [21] envisioned and investigated an all-IP network architecture integrating mobility, Quality of Service (QoS), AAA support based on IPv6, and charging for services. The architecture provides seamless hand-over support across heterogeneous access technologies, and considers different administrative domains. The accounting functionality is based on the IETF AAA architecture with Diameter and the RTFM (Real-time Traffic Flow Measurement) meter [10]. The follow-up project, Daidalos [14] develops an open architecture focusing on personalized services. The goal is to seamlessly integrate heterogeneous network technologies, and to provide pervasive and user-centered access to services, where accounting and charging play a central role. The latter issues are enhanced with a proposal on pre-paid charging models in an all-IP networking environment.

Considering the telecommunication world, the 3rd Generation Partnership Project (3GPP) [6] comprises standardization bodies in order to develop technical specifications for a 3rd generation mobile system. 3GPP defines standards for the UMTS network from the radio access technologies up to network architecture and management processes. As all commercial networks, UMTS also includes various support for accounting and charging functionality described in the next section in detail.

3 Background Technology

An overview and analysis of accounting functionality in current networks is of importance for the design of the integrated accounting architecture. First the accounting infrastructure for UMTS is discussed, followed by the infrastructure for WLAN.

3.1 Accounting and Charging in UMTS

UMTS is the next generation mobile telecommunication system providing higher data transfer rates, QoS support and an infrastructure for services provisioning. UMTS is a step towards the convergence of the telecommunication and the IP world.

The UMTS network consists of the UMTS Terrestrial Radio Access Network (UTRAN) and the Core Network (CN) [3]. The UTRAN implements the radio interface towards the mobile devices, and it is responsible for the wireless transmission. The UTRAN includes NodeBs forming radio cells and providing the radio interface, and Radio Network Controllers (RNC) coordinating the NodeBs. The RNC also provides the connection between UTRAN and CN. The Core Network is subdivided in the circuit switched (CS) and the packet switched (PS) domain. The main network components in the PS domain are the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN) [2]. They are responsible for access control, packet switched data transfer and mobility management. The GGSN connects the UMTS network to external packet switched networks like the Internet, and the SGSN provides the interface towards the UTRAN.

Figure 1 illustrates the architecture of a UMTS network focusing on the accounting functionality in the PS domain for postpaid charging. The description in this paper is based on Release 5.

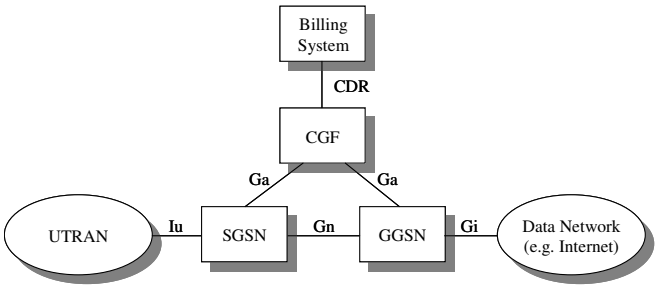

Figure 1: UMTS charging architecture

The SGSN and GGSN collect accounting information separately for each individual PDP (Packet Data Protocol) context. This contains the system and resource usage of active users. The Charging Gateway Function (CGF) collects accounting data from the SGSN and GGSN via the Ga interface, and transfers it to the billing system in the form of Charging Data Records (CDR). The CGF can either be implemented as a separate network component or its functionality can be integrated in the GSNs. The CGF buffers the received CDRs in a local storage. Before forwarding CDRs to the billing system, the CGF can correlate CDRs, extend them with additional, billing system specific information, or remove not required CDR attributes. The CGF can support several protocols in order to enable interworking with different billing systems. The billing system is responsible to prepare the final monthly invoice for mobile network subscribers.

To allow the correlation of CDRs belonging to the same PDP context, a unique charging ID is used by the GSNs. The charging ID is generated by the GGSN, which is assigned for the whole PDP context lifetime, while the SGSN can be changed. This allows the consolidation of CDRs also in case of mobile users changing his point of attachment along with the current SGSN.

Charging data records contain accounting information about service and resource usage required for charging and billing. There are different types of CDRs depending on the network component generating them and the purpose of the record. The S-CDR generated by the SGSN and the G-CDR generated by the GGSN contain information related to a PDP context. Additionally, the SGSN generates the M-CDR for mobility management information, the S-SMO (Short message Mobile Originated), and S-SMT (Short message Mobile Terminated) for the SMS (Short Message Service) service. The latter ones are not considered in more detail.

The CDR includes attributes among others to identify the user and his device, i.e. IMSI (International Mobile Subscriber Identity), IMEI (International Mobile Equipment Identity); the network elements providing the service, i.e. GSN addresses; as well as information about the service usage, e.g. List of Traffic Data Volumes, APN (Access Point Name), Served PDP address. Additionally, the record can include location information like routing and location area codes and cell ID. The List of Traffic Data Volumes attribute provides information about the resource usage, and it consists of one or more containers with the following fields:

- Data volume uplink and downlink

- Change condition and change time
- QoS requested and QoS negotiated (optional fields)

Table 1 shows the most important attributes in the S-CDR as an example. This list is not fully exhaustive, however, for the complete list and also for the other types of CDRs refer to [4]. The G-CDR, generated by the GGSN, is almost identical to the S-CDR. Some of the attributes are mandatory, conditional, or operator specific, but they are not specified explicitly in the table.

Table 1: S-CDR attributes

Attribute Name	Description
Record Type	Type of the CDR, in this case S-CDR.
Served IMSI	The IMSI of the served party.
Served IMEI	The IMEI of the mobile equipment.
Served MSISDN	The primary MSISDN of the subscriber.
SGSN Address	The IP address of the current SGSN.
GGSN Address	The IP address of the current GGSN.
Charging ID	An identifier used to correlate records created by different GSNs.
Charging Characteristics	The charging characteristic (e.g. postpaid, prepaid) applied to the PDP context.
APN Network ID	The network identifier part of the APN.
APN Operator ID	The operator identifier part of the APN.
PDP Type	Type of the PDP context, e.g. IP, PPP.
Served PDP Address	PDP address of the served device, i.e. IPv4 or IPv6 address.
List of Traffic Data Volumes	A list of the resource usage and changes of charging conditions for the PDP context.
Record Sequence Number	Partial record sequence number in the SGSN
Record Opening Time	Time stamp when the PDP context is activated in the SGSN.
Duration	Duration of this record in the SGSN.
Cause for Record Closing	The reason for closure of the record from the SGSN.
Routing Area Code	Routing area code at “Record Opening Time”
Location Area Code	Location area code at “Record Opening Time”
Cell Identifier	Service area code for UMTS at “Record Opening Time”

A container includes accounting data for the duration when PDP context conditions, e.g., QoS, tariff, do not change. Every time conditions change, a new container is opened, and accounting data is collected separately according to the new conditions.

CDRs are transferred via the Ga interface using the GTP’ protocol [4], which is based on the GPRS Tunneling Protocol (GTP) [1]. The protocol supports the transfer of CDRs, redirection to another CGF, detection of communication failures, and preventing duplicate CDRs.

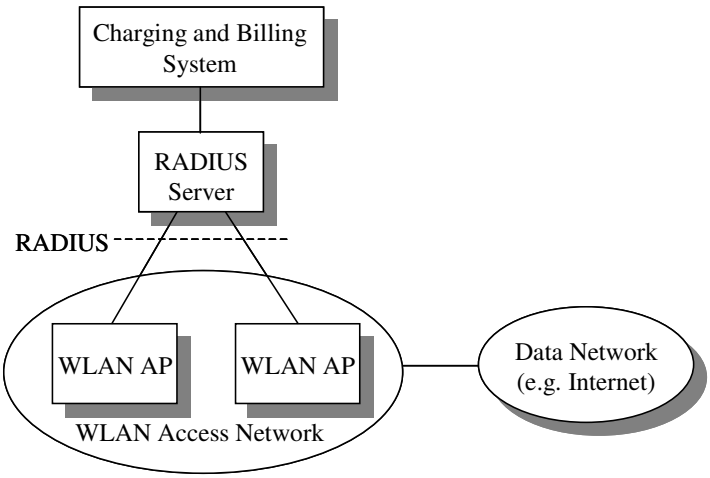

Figure 2: Accounting in WLAN based on RADIUS

3.2 Accounting and Charging in WLAN

Figure 2 shows the typical network components deployed in current WLAN networks. The access network consists of WLAN access points providing connectivity to mobile devices via the radio interface. Current access points usually support AAA functionality based on the RADIUS protocol. This allows together with a RADIUS server to control the access of mobile users to the network, and to collect accounting information for individual users. After successful user authentication and authorization, the WLAN access point (AP), acting as a RADIUS client, collects accounting data on the resource usage of the user. This data is communicated to the RADIUS server after the user terminates the service. The AP can also send accounting data during an active session to the server in interim accounting records in order to improve reliability. The server stores the records in a database for further processing. Similar to the UMTS network, the charging and billing system is responsible for the charge calculation and to prepare the final monthly invoice for the subscribers.

RADIUS accounting supports the collection of usage-data summarized in Table 2. The list provides only the most important attributes serving accounting purposes as an example. The complete attribute list is specified in [26] and [25]. The attributes allow to account for the transferred data volume, the number of packets separate in both directions, and the session duration. Additionally to the attributes listed in the table, RADIUS also supports to transfer other information applicable for accounting like user name, IP address, service type, NAS identifier or NAS port type.

Table 2: RADIUS accounting attributes

Attribute Name	Description
Acct-Status-Type	Indicates the type of the packet, e.g. start, stop.
Acct-Session-Id	ID to uniquely identify a session.
Acct-Multi-Session-Id	ID to link multiple related sessions together.
Acct-Session-Time	Indicates the connection time of a user.
Acct-Input-Octets	Number of incoming octets during a session.
Acct-Output-Octets	Number of outgoing octets during a session.
Acct-Input-Packets	Number of incoming packets during a session.
Acct-Output-Packets	Number of outgoing packets during a session.
Acct-Terminate-Cause	The reason for the termination of a user's session.

4 A Multi-domain, Multi-technology Scenario

In the multi-domain, multi-technology scenario shown in Figure 3, network operators provide network access to their customers via different access technologies. In the scenario the two most promising wireless access technologies, both enabling mobile communication, are considered. One of them is the next generation mobile telecommunication system, UMTS, and the other is the fast evolving WLAN. Network operators participating in the scenario include traditional mobile telecommunication companies operating a UMTS network, and operators providing IP access in WLAN hotspots like at airports or in hotels. Additionally, mobile network operators can also have a WLAN network infrastructure beside their UMTS network as illustrated in Figure 3 for network operator *A*. The scenario focuses on the provisioning of IP connectivity to the Internet, thus, in case of UMTS only the packet-switched domain is addressed. Among those operators an interconnection network provides network connectivity. This can be the Internet, but also a dedicated network like GRX (GPRS Roaming Exchange) in case of today's GSM networks.

On one hand, beside the network connection, operators also have roaming agreements with each other in order to allow for their customers to attach to the network of other operators. On the other hand, users have a contract with one of those operators, this particular one is termed their home operator. The home operator prepares the monthly invoice, and also supervises and controls the payment process.

Users can get access to UMTS and WLAN networks via appropriate end devices supporting both access technologies. The network infrastructure allows mobile users to keep attached also on the move.

Figure 3 shows different hand-over scenarios. Hand-overs can take place within the same access technology, i.e. from base station to base station in UMTS, or from an access point to another access point in WLAN. This is referred to as horizontal hand-over. Vertical hand-overs, on the other hand, occur between different access technologies, e.g., from UMTS base station to a WLAN access point. If the hand-over is performed between two network operators it is referred to as roaming. In this multi-domain, multi-technology scenario the charging process has to be supported by an integrated accounting infrastructure that provides a common and technology-independent interface, and enables accounting for different access technologies also during hand-over.

Scenario No. 1 and 3 in Figure 3 show a horizontal hand-over in UMTS and WLAN respectively within one operator's domain. In this case the accounting process has to be able to collect accounting data during the hand-over, and has to be able to associate it to the same user session. Scenario No. 2 illustrates a vertical hand-over from UMTS to WLAN within one operator's domain. In this case the accounting process has to support the switching over between different technologies, which includes the collection of individual accounting parameters in new network components by technology dependent mechanisms. The correla-

tion of UMTS and WLAN access sessions has to be supported as well. In case of a vertical hand-over, the hand-over decision is based not only on current coverage and availability of a given technology, but also on the characteristics of the access technology and on economical aspects like price as well. WLAN access has most likely lower access fees and higher data transfer rates as UMTS, but the latter one provides QoS for example. Finally, scenario No. 4 shows a roaming scenario between operator *A* and *B*, where additionally to the previous scenarios collecting and transferring of accounting information between different operators has to be possible. This process raises also security issues. The hand-over can take place within the same or between different access technologies, and again hand-over is not only influenced by technical means, but also by economical aspects like higher roaming prices.

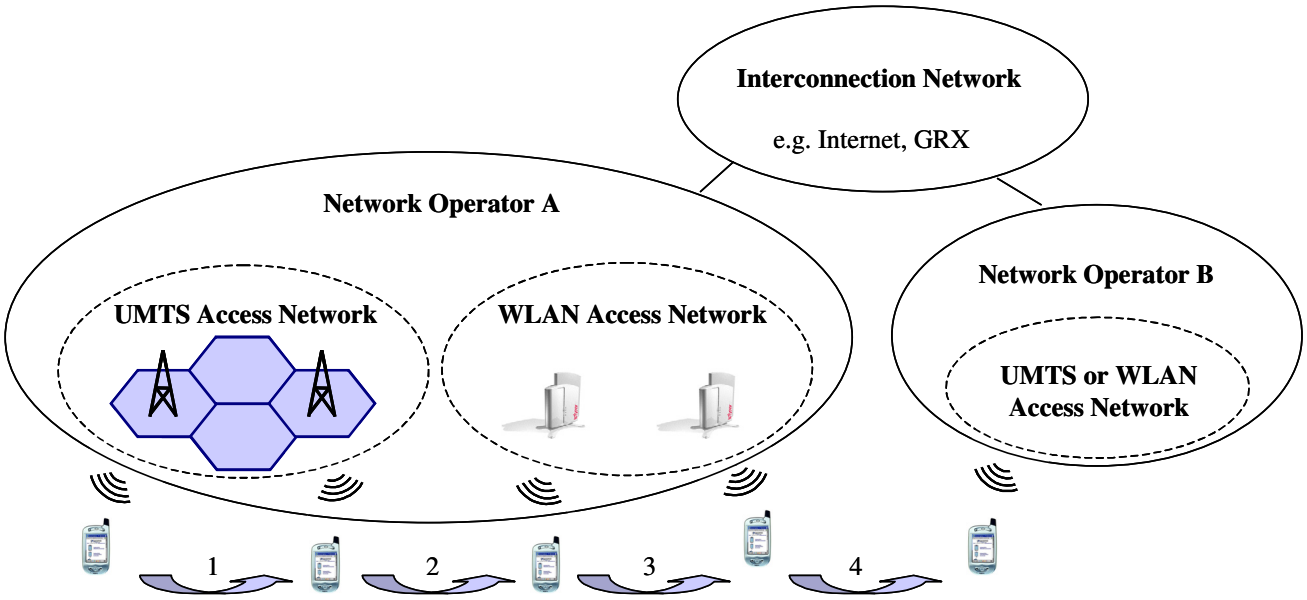

Figure 3: Multi-domain, multi-technology scenario

Summarizing the key requirements that those scenarios define, a distributed accounting architecture for charging in mobile networks with heterogeneous access technologies in a multi-domain environment has to support the collection of usage-data for different technologies across operator domains in a common and consistent manner. It has to provide suitable and available accounting parameters and accounting data records for heterogeneous networks. The architecture has to enable accounting also during hand-over, and consider security issues between operator domains. Additionally, the system has to fulfil also general requirements. This includes that the accounting process should be scalable and efficient. The system has to provide interoperability, i.e. it has to use standard protocols, and be able to be integrated into existing systems in order to minimize implementation efforts. Finally, accounting records have to provide service-specific attributes, and they have to allow extensions according to future or application specific requirements.

5 Integrated Accounting for UMTS and WLAN Networks

The integrated accounting architecture defines all extensions required in network components and in the Diameter protocol in order to allow for the transfer of UMTS and WLAN specific accounting data in a common form. Diameter [12] is chosen as general accounting protocol determining the basis for the architecture. The protocol fulfils the accounting functionality required in both networks. It has a flexible AVP structure, which can be extended to support the transfer of additional accounting attributes required in UMTS and WLAN.

Diameter also provides the same functionality as the current accounting protocol GTP' [1] does within UMTS. It supports reliable transfer of accounting data, it can detect communication failures, it has a flexible routing mechanism with redirection functionality, and it supports failover mechanisms. Additionally, GTP' messages can be mapped to Diameter accounting messages. All these steps enable Diameter to replace the GTP' protocol in UMTS accounting.

Diameter can also be deployed in WLAN networks replacing RADIUS [26], because backwards compatibility was already considered in the design. Additionally, because Diameter is based on the widely deployed RADIUS protocol, the acceptance of Diameter is supposed to become high. Thus, Diameter is a promising candidate to be a common accounting protocol.

5.1 Network Architecture

All network components and their interfaces for the integrated accounting architecture are shown in Figure 4. Although the figure illustrates only one entity for each kind of network components, several accounting servers, SGSNs, GGSNs, and WLAN APs are most likely deployed in a network. The Diameter clients can communicate with the server via other Diameter nodes

(e.g., relay, proxy) as specified in the Diameter base protocol [12]. This makes the architecture also valid for more complex networks, enabling communication also across domains. But for simplicity only one Diameter server will be shown in next figures.

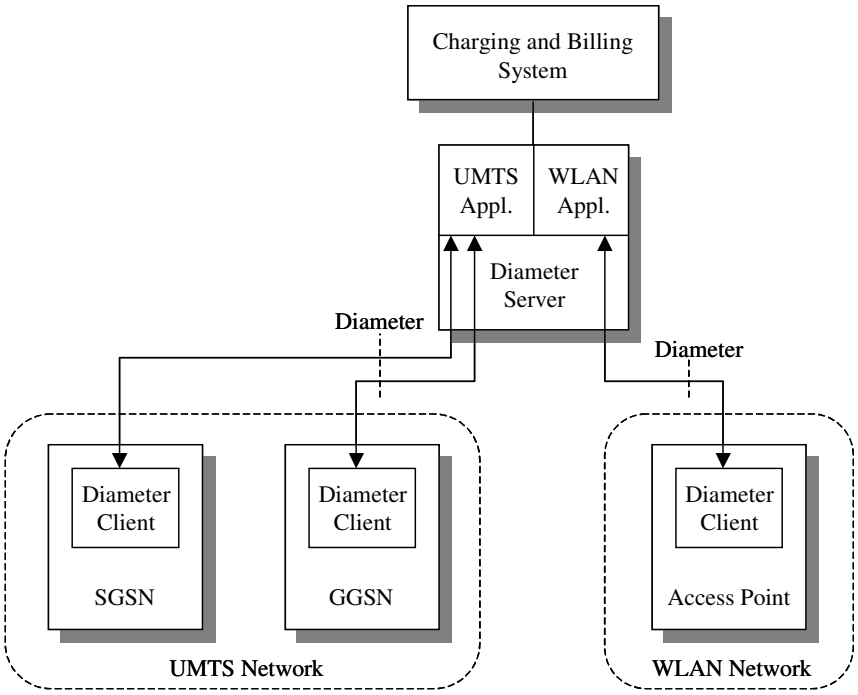

Figure 4: Integrated accounting architecture

The CGF is replaced by a common Diameter server, which is responsible for the accounting process both in UMTS and WLAN access networks. The GSNs are extended with a Diameter client, and the WLAN access points also support accounting based on Diameter. Clients collect accounting information on service and resource usage, and report it to the accounting server. The server in turn stores accounting records, which provide the input for the charging and billing system. The communication between accounting entities is completely based on the Diameter protocol, thus GTP' in UMTS is completely replaced. The accounting server supports two separate Diameter applications for UMTS and WLAN. This allows for an independent definition of separate accounting attributes and messages for different access technologies, and for an extension of the accounting server with the support of new technologies without the change of other applications. Separate Diameter applications can handle different technologies by separate accounting processes. The charging and billing system takes accounting data from the Diameter server, calculates the charges for service usage, and prepares the final invoice.

Figure 5 shows the network architecture for a migration scenario, enabling currently deployed and standard equipment to be integrated into the proposed accounting architecture. GSNs support only the standard Ga interface with the GTP' protocol, and a Diameter translation agent takes over and handles the conversion between GTP' and Diameter protocol messages. Similarly, a translation agent connects RADIUS-based access points to the integrated Diameter accounting server. The translation agents connect heterogeneous networks, and provide the interface between accounting protocols. The architecture allows for a combination of the migration scenario with the pure Diameter solution shown in Figure 4.

The integrated accounting server enables the processing of accounting information for UMTS and WLAN in a common way, and the correlation of accounting data from both networks. The common server can also account for services across hand-overs within and between different access technologies, and it provides a generic interface toward the charging and billing system.

5.2 Accounting Parameters

Table 3 defines the Diameter AVPs that are required to be able to transfer UMTS specific accounting data by the Diameter protocol. The first column of the table contains those attributes specified for the UMTS S-CDR and G-CDR shown in Table 1, the second column lists the corresponding Diameter AVPs defined for the proposed accounting architecture, and the third column specifies AVP value types. Those attribute value types correspond to the types specified by the Diameter base protocol [12]. Most of these attributes are defined as new AVPs, but some of them can be mapped to already specified Diameter AVPs [13]. Thus, Data Volume Uplink is mapped to Accounting-Input-Octets, Data Volume Downlink to Accounting-Output-Octets, Duration to Acct-Session-Time.

According to the specification of the UMTS accounting container, Traffic-Data-Volume is a grouped AVP and contains the following AVPs, each included exactly once:

- Accounting-Input-Octets,
- Accounting-Output-Octets,
- Change-Condition, and

- Change-Time.

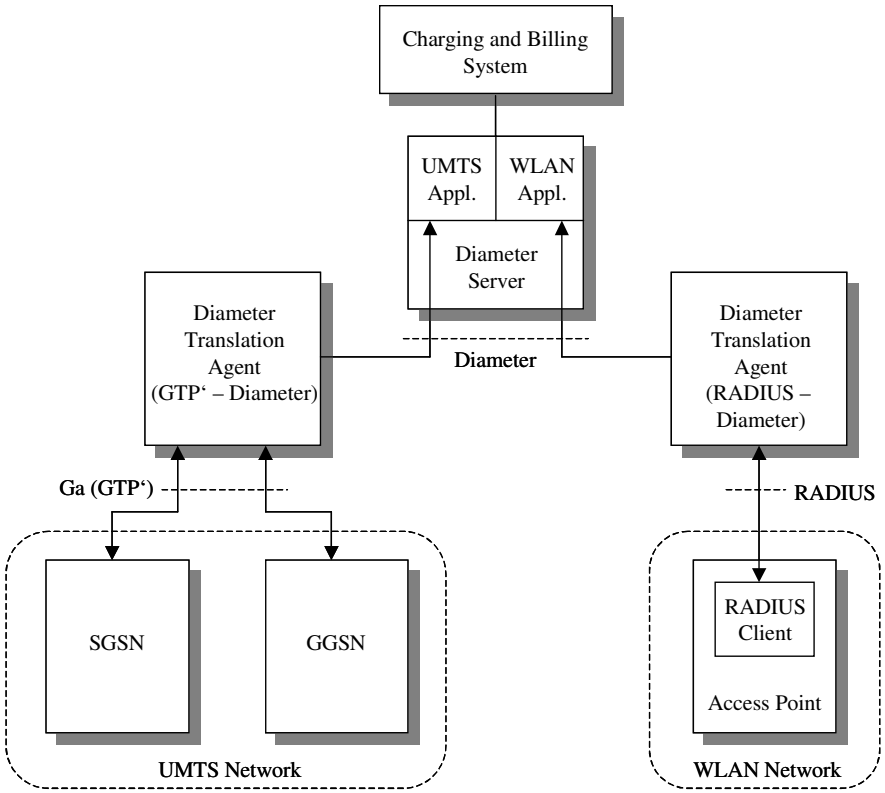

Figure 5: Migration accounting architecture

Additionally, Traffic-Data-Volume can include the following optional AVPs:

- QoS-Requested, and
- QoS-Negotiated.

Those AVPs defined are mandatory, thus, they have to be supported by the Diameter application, and the mandatory flag must be set for them in accounting messages. But this does not mean that all accounting messages must include all AVPs. The P bit for encryption may be set.

Additionally to those AVPs defined by the Diameter base protocol, the following AVPs must be present in accounting requests with Record-Type=S-CDR according to [4]:

- Record-Type,
- Served-IMSI,
- Charging-Id,
- GGSN-Address,
- Record-Opening-Time,
- Acct-Session-Time,
- Cause-For-Record-Closing,
- Charging-Characteristics.

If the Record-Type is equal to G-CDR, the following AVPs must be included in accounting requests:

- Record-Type,
- Served-IMSI,
- Charging-Id,
- SGSN-Address,
- GGSN-Address,
- Record-Opening-Time,
- Acct-Session-Time,
- Cause-For-Record-Closing,
- Charging-Characteristic.

All other AVPs are specified as optional, and can be included in accounting requests. The complete list of AVPs for accounting messages and for different types of CDRs can be defined analogously, according to the specifications of [4].

The assignment of AVP value types is based on the type definition of UMTS attributes in [4]. All AVPs required for UMTS are matched based on their types to those data types defined for CDRs to make a conversion as easy as possible later on. But some of those UMTS attributes have a partitioned structure, which can be applied also for the Diameter AVPs, or they can be mapped to more than one AVP. Additionally, the value type of an AVP can be specified for some attributes different as it is for UMTS. The Charging Characteristics is a good example here, which is defined as a bit-field in CDRs, but in Diameter it could be specified as an AVP of type enumerated. This shows that the mapping of accounting attributes is not explicit, but it is a design decision.

Table 3: Diameter accounting AVPs for UMTS

Attribute Name	Diameter AVP	Value Type
Record Type	Record-Type	OctetString
Served IMSI	Served-IMSI	OctetString
Served IMEI	Served-IMEI	OctetString
Served MSISDN	Served-MSISDN	OctetString
SGSN Address	SGSN-Address	Address
GGSN Address	GGSN-Address	Address
Charging ID	Charging-Id	Unsigned32
Charging Characteristics	Charging-Characteristics	OctetString
APN Network ID	APN-Network-Id	UTF8String
APN Operator ID	APN-Operator-Id	UTF8String
PDP Type	PDP-Type	OctetString
Served PDP Address	Served-PDP-Address	OctetString
List of Traffic Data Volumes	Traffic-Data-Volume	Grouped
QoS Requested	QoS-Requested	OctetString
QoS Negotiated	QoS-Negotiated	OctetString
Data Volume Uplink	Accounting-Input-Octets	Unsigned64
Data Volume Downlink	Accounting-Output-Octets	Unsigned64
Change Condition	Change-Condition	Enumerated
Change Time	Change-Time	OctetString
Record Sequence Number	Record-Sequence-Number	Unsigned32
Record Opening Time	Record-Opening-Time	OctetString
Duration	Acct-Session-Time	Unsigned32
Cause for Record Closing	Cause-For-Record-Closing	Unsigned32
Routing Area Code	Routing-Area-Code	OctetString
Location Area Code	Location-Area-Code	OctetString
Cell Identifier	Cell-Id	OctetString

In the proposed accounting architecture the session concept of Diameter is applied, thus, all accounting messages include also the Session-Id AVP. The Charging-Id is included only for compatibility reasons. The Diameter accounting AVPs required for the WLAN application are listed in Table 4. They are defined according to [12] and [13].

Table 4: Diameter accounting AVPs for WLAN

Attribute Name	Diameter AVP	Value Type
Acct-Status-Type	Accounting-Record-Type	Enumerated
Acct-Session-Id	Acct-Session-Id	OctetString
Acct-Multi-Session-Id	Acct-Multi-Session-Id	UTF8String
Acct-Session-Time	Acct-Session-Time	Unsigned32
Acct-Input-Octets	Accounting-Input-Octets	Unsigned64
Acct-Output-Octets	Accounting-Output-Octets	Unsigned64
Acct-Input-Packets	Accounting-Input-Packets	Unsigned64
Acct-Output-Packets	Accounting-Output-Packets	Unsigned64
Acct-Terminate-Cause	Termination-Cause	Enumerated

Basic guidelines for a RADIUS/Diameter protocol translation are also specified in [13]. According to that, a translation agent forwarding a RADIUS accounting request as a Diameter request has to convert some of the AVPs. The Acct-Status-Type attribute must be converted to Accounting-Record-Type. If the accounting message contains the Acct-Termination-Cause attribute,

it must be converted to the Diameter Termination-Cause AVP. Finally, Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets, and Acct-Output-Packets must be converted to the Diameter 64-bit equivalent AVPs.

For a session identification the Diameter Session-Id AVP is used, which is created by the Diameter client in the WLAN access point or by the Diameter translation agent. The Acct-Session-Id attribute in Diameter is only included for compatibility, and it is only used in case of a RADIUS/Diameter protocol translation. It contains then the RADIUS Acct-Session-Id.

5.3 Accounting Process

The accounting process describes the interactions between the related network components. Figure 6 shows the accounting process in a UMTS network. The process is divided into three phases. The first is the PDP context establishment together with the start of accounting. The second phase shows the possible accounting messages during an active connection, and the third describes the PDP context release and the termination of accounting. UMTS related signaling messages for PDP context establishment, modification, and release are only shown between the SGSN and GGSN, and they only indicate the relation between the accounting process and UMTS signaling.

After the SGSN authorized the request for PDP context establishment, it sends a Create PDP Context Request message to the GGSN. The GGSN in turn also authorizes the connection, and checks whether the required resources can be allocated. If the GGSN allows the connection establishment, it creates a Diameter Session-Id and also a Charging-Id for the connection. Then the Diameter client within the GGSN sends an Accounting-Request (ACR) message with the Accounting-Record-Type AVP set to START_RECORD to the accounting server. The server updates its internal state, and sends an Accounting-Answer (ACA) back to the client. The answer contains an Acct-Multi-Session-Id, which must be included in all further messages by the client. This ensures that the server can correlate accounting records belonging to the same session, but coming from different network components. This also enables to maintain the correlation across hand-overs. After receiving the Create PDP Context Response, the SGSN also starts accounting, and sends an ACR message to the server. It receives in the ACA message the same Acct-Multi-Session-Id from the server as the GGSN.

The accounting messages can be forwarded or redirected by Diameter agents also across domains to different servers according to standard Diameter mechanisms. The message routing is based on realms identified in the Destination-Realm AVP. This allows for finding a responsible server for the current user, which will coordinate the accounting process. Based on a user and network operator identifier, the Diameter node creating the request can fill in the Destination-Realm AVP. In case of UMTS the identifier can be the IMSI, and in case of WLAN the realm portion of the user name.

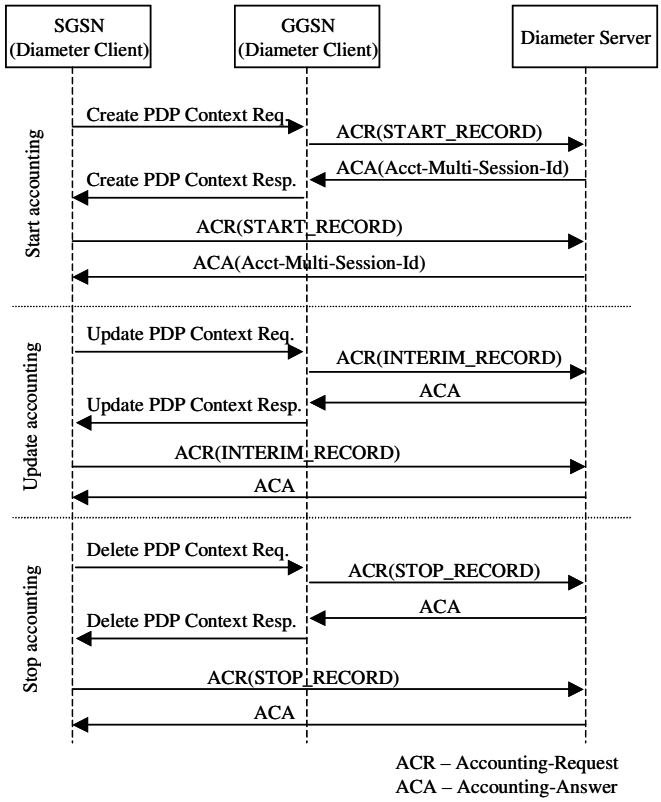

Figure 6: Accounting process for UMTS

In the second phase of the accounting process, GSNs can send ACR messages with interim records to the server, based on a PDP context modification as shown in Figure 6. Interim records can also be sent periodically with a given interval, or based on a change condition defined in Section 3.1. According to the different CDR types, ACR messages contain the AVPs defined in the previous section.

During a connection release the SGSN sends a Delete PDP Context Request to the GGSN. According to the request, the GGSN terminates the PDP context, and sends an ACR message with record type set to STOP_RECORD to the server. Additionally, the GGSN replies with a Delete PDP Context Response to the SGSN, which in turn also stops accounting, and reports the collected usage data for the PDP context in an ACR message to the server.

The UMTS hand-over scenario, where the associated SGSN is also changed, is illustrated in Figure 7. It is assumed that the PDP context is already established, and accounting is also started as described above. As the mobile node moves to a cell associated to a new SGSN, the PDP context is updated and switched to the new SGSN. After the context exchange between the old and new SGSNs, the old SGSN sends an ACR message with a stop record containing the required accounting parameters to the server. The new SGSN informs the GGSN about the hand-over and the PDP context modification with an Update PDP Context Request message. Hereon, the GGSN sends an ACR interim message to the accounting server to get the hand-over event be recorded. After receiving the Update PDP Context Response, the SGSN is ready to serve the mobile node, and it starts accounting sending an ACR start record to the server. In the response it receives the same Acct-Multi-Session-Id as the one assigned to the old SGSN and to the GGSN. This enables the accounting server to correlate accounting records from the new SGSN to the same accounting session as used before the hand-over. How to find the same server is discussed later in this section. Afterwards, the accounting process can be continued with the phases update or stop accounting as illustrated in Figure 6, and described above.

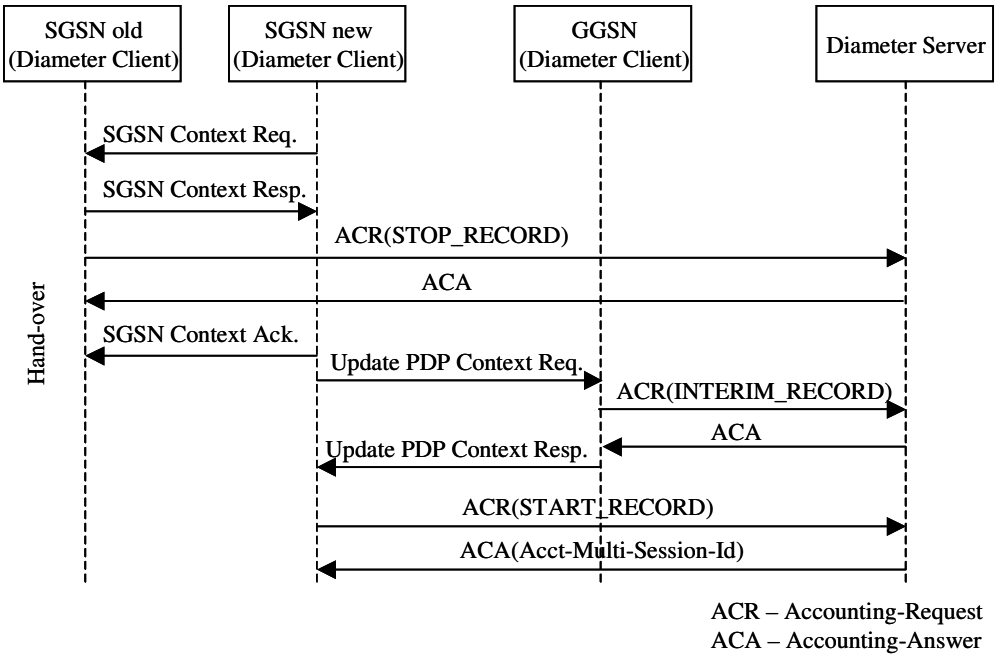

Figure 7: Accounting process for hand-over in UMTS

Besides primary PDP contexts considered so far, the UMTS architecture allows for the establishment of secondary PDP contexts, which are always associated to a primary PDP context. To account for secondary PDP contexts, the Accounting-Sub-Session-Id is used. It identifies the secondary PDP context, and allows for assigning it to a primary one with a unique Session-Id.

For the accounting of SMS transmission via the SGSN, the SGSN uses the SGSN mobile originated SMS record (S-SMO-CDR) and the SGSN mobile terminated SMS record (S-SMT-CDR) depending on the sending direction. The SGSN reports the SMS transmission to the accounting server in an ACR message with record type set to EVENT_RECORD. The accounting event record fits best for an SMS service, because it is used to indicate a one-time event, and the record contains all information relevant to the service.

The accounting process for a WLAN network is shown in Figure 8. The process is similarly divided into several phases as in case of UMTS, but it already includes the messages in case of a hand-over. After the user is attached to a WLAN AP, and successfully authenticated and authorized, the Diameter client within the WLAN AP sends an ACR start message, and starts collecting required accounting data. The accounting server responds with an ACA message including an Acct-Multi-Session-Id. The purpose of this Id is the same as in the case of UMTS, namely to enable the correlation of accounting data across hand-overs.

In the second phase the WLAN AP can send interim records to the server in order to update the collected accounting information. The interval of the periodical update can be controlled by the server using the Acct-Interim-Interval AVP. Accounting records in ACR messages include accounting attributes defined in Table 4.

In case of a hand-over within the WLAN network, the old access point stops accounting, and sends an ACR stop record containing the collected usage data to the server. On the other hand, the new access point, the user attached to, starts accounting by sending an ACR start record to the Diameter server. The client receives the same Acct-Multi-Session-Id as used before the hand-over, which must be included in all further accounting messages.

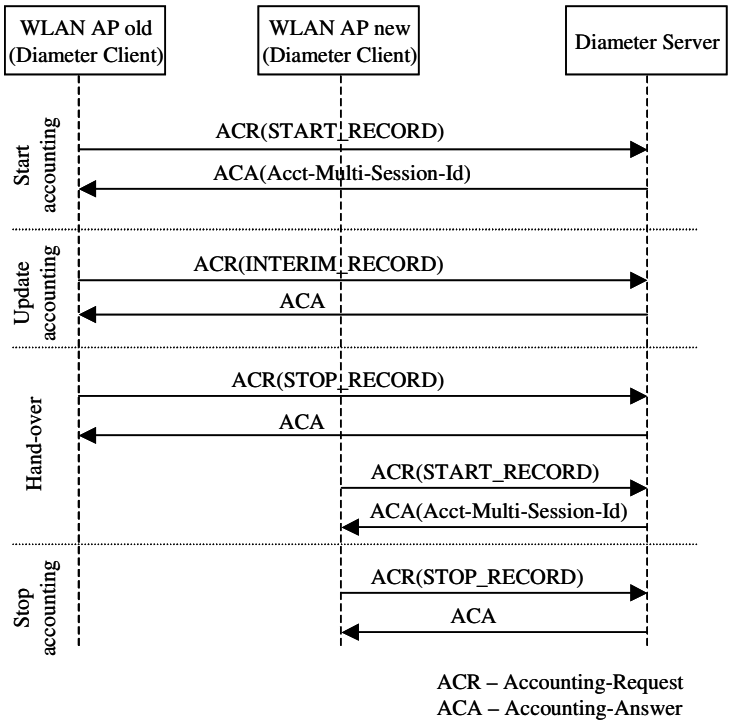

Figure 8: Accounting process for WLAN

The accounting process during hand-over must be assisted by the mobility management in order to be able to find the same Diameter server, which coordinates the accounting process, and to inform it about the user sessions belonging together. The exact sequence of the accounting messages shown in Figure 8 also depends on the applied mobility management. In the proposed Diameter mobile IPv4 application [11] the mobile node must support the AAA NAI (Network Access Identifier) extension [8], [17] in order to be able to route the AAA messages to the same AAA server to which the user currently registered. The mobile node must include the AAA NAI in registration messages when changing its point of attachment. The Diameter client in the new AP includes the Destination-Host AVP in the request message containing the AAA NAI received from the mobile node, which ensures that the message will be routed to the same server. This approach is applied also in the proposed accounting architecture to enable the correlation of accounting sessions across hand-overs. In case of UMTS, the SGSN can receive the AAA NAI also from the GGSN in the Create and Update PDP Context Response messages.

Combining those accounting processes defined for UMTS and WLAN networks above, Figure 9 shows the accounting messages for a hand-over from UMTS to WLAN. After the mobile node is attached to the WLAN AP, the accounting process is terminated in the UMTS network, and it is started in the WLAN network as described above. Again, the Acct-Multi-Session-Id provides the means to associate the accounting sessions in the two access networks. The exact order of the messages depends on the applied mobility management, which has to assist the accounting process.

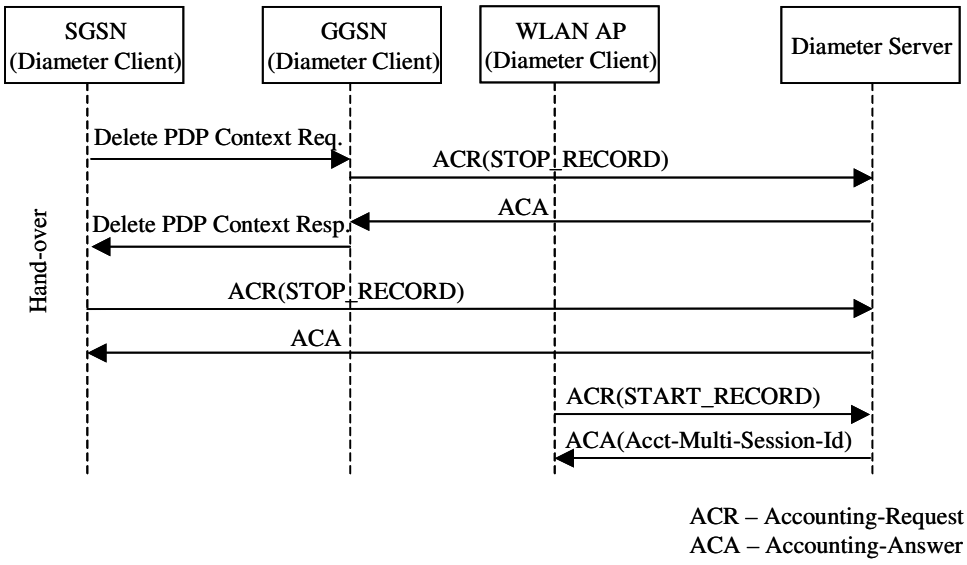

Figure 9: Accounting process for hand-over from UMTS to WLAN

In case of the migration scenarios discussed in Section 5.1, the Diameter translation agent takes the role of the Diameter clients deployed in GSNs and WLAN APs. The agent provides the same interface towards the Diameter server as described above, which makes it transparent to the server. Agents can convert between different accounting protocols applied in the architecture. This includes the translation between GTP' and Diameter, and RADIUS and Diameter. In addition to the protocol conversion, agents maintain internal state information in order to be able to assign GTP' and RADIUS connections to Diameter accounting sessions. The state information contains the mapping between different session identifiers used by the accounting protocols. These include the Charging Id for GTP', the Acct-Session-Id for RADIUS, as well as the Session-Id and Acct-Multi-Session-Id for Diameter.

In a multi-domain environment also security issues arise. The Diameter base protocol provides a security framework to exchange messages in a secure manner based on IP Security (IPSec) [18] and Transport Layer Security (TLS) [15]. Furthermore, it recommends to use TLS when the connection between Diameter peers is crossing operator domains. Therefore, on each connection authentication, integrity, confidentiality and replay protection is in place on a per-packet basis. The Diameter protocol also supports end-to-end security services including confidentiality and message origin authentication, enabling the secure connection between two peers communicating through agents. The security mechanisms can be based on certificates or pre-shared keys. Additionally to the technical aspects, roaming agreements, business and trust relations determine the possibility for an inter-domain communication.

6 Implementation and Evaluation

The prototype implementation of the proposed integrated accounting architecture is based on Open Diameter in version 1.0.7-a [22], [23]. Open Diameter is an open source project hosted by SourceForge with the aim to implement the Diameter protocol. The project is still under development, and the implementation currently provides libraries with basic Diameter functionality, but a stand-alone Diameter client, server or agents are not implemented yet. This implementation relies on several other frameworks not explained at this stage in detail. Because of the open source nature of Open Diameter, it is the right choice for the prototype, enabling to implement all defined extensions.

The Diameter base protocol and Diameter applications are separated in Open Diameter, and new applications can be added as modules to the framework. The proposed extensions are implemented as separate Diameter applications allowing to keep the base protocol unchanged.

The Open Diameter configuration files use XML as an encoding language in general. Diameter messages and AVPs are defined in the dictionary.xml configuration file. The file serves as input for the parser to identify attributes when creating or parsing a message. The prototype implementation extends Open Diameter with additional AVPs as defined in Table 3 and Table 4. All codes assigned to AVPs are allocated by IANA (Internet Assigned Numbers Authority), but for the prototype those code numbers were selected, which are not conflicting with existing ones. At a later stage, they could be assigned by IANA or specified as vendor-specific.

Figure 10 illustrates the XML syntax for the definition of Diameter messages and AVPs in Open Diameter. The figure shows the Accounting-Request and Accounting-Answer commands as an example. The message structure of the request is specified with the `<requestrules>` tag. Similarly, the `<answerrules>` tag specifies the answer. Firstly, AVPs with a fixed position are defined. There is actually one AVP defined with a fixed position, which is the Session-Id. Secondly, AVPs which must be included in the message (mandatory), are specified as required. Last, optional AVPs follow. Figure 10 also shows the definition of the Served-IMSI AVP as an example. Command code 911 is assigned to it, and it is a mandatory AVP, which may be encrypted. The value type is OctetString. The other AVPs defined in Table 3 and Table 4 are specified similarly.

The stand-alone Diameter client and server implementations are based on examples included in Open Diameter for test purposes. They are extended to provide the required accounting functionality. The client can send accounting messages with start, interim, stop, or event records. Metering is not integrated into the client, thus, accounting parameters are filled with arbitrary default values. The server is an application that reacts to incoming messages and sends the appropriate Diameter answer back to the client. Additionally, the server translates incoming messages together with the accounting data into an XML document, which is used to verify the correct transfer of data.

To evaluate the implementation, a test-bed with a client and server application installed on two separate machines was used. The test was focused on a functional evaluation verifying the message handling and data transmission functionality between client and server, and the correct processing of the defined AVPs. In the test scenario, on one hand, the client establishes several parallel accounting sessions, and sends accounting records both for UMTS and WLAN. The server, on the other hand, maintains accounting sessions, responds to requests coming from the client, and saves messages together with accounting data in a separate file for each session.

The implementation demonstrates that the proposed integrated accounting architecture can be completed and Diameter can be extended to support accounting functionality in UMTS and WLAN environments in a common and integrated manner. The tests performed show that the client and server applications communicate correctly, and they can exchange the required accounting data. The server manages accounting sessions, and correctly assigns accounting records to the right session. The Diameter routing functionality in Open Diameter is not completely implemented yet, thus, it is not able to handle message routing properly at this stage.

```
<command name="Accounting" code="271">
 <requestrules>
  <fixed>
   <avprule name="Session-Id" maximum="1" minimum="1" />
  </fixed>
  <required>
   <avprule name="Origin-Host" maximum="1" minimum="1" />
   ...
  </required>
  <optional>
   <avprule name="Acct-Multi-Session-Id" maximum="1" minimum="0" />
   ...
  </optional>
 </requestrules>
 <answerrules>
   ...
 </answerrules>
</command>

<avp name="Served-IMSI" code="911" mandatory="must" protected="may" may-encrypt="yes">
  <type type-name="OctetString"/>
</avp>
```

Figure 10: Definition of Diameter messages and AVPs

Besides the functional evaluation, those tests also delivered some initial performance results of the current Open Diameter implementation. The processing of accounting start messages resulting in a new session establishment in the server is significantly slower than processing other types of messages. To illustrate this, in the situation of the establishment of 500 simultaneous sessions, the client is not able to establish about 5% of those sessions. If the server has to process parallel other messages as well, the error ratio becomes even higher. The delay between request and response at the client can exceed 20 seconds in some cases.

7 Summary and Conclusions

Accounting and charging for service and resource usage are two of the key tasks to be performed within commercially operated networks. With emerging new access technologies and the increasing number of mobile users, the need for a common accounting process becomes higher in order to reduce operational costs and management efforts. Based on a detailed analysis of current accounting mechanisms in UMTS and WLAN, a new approach is presented based on the Diameter protocol, enabling to process accounting data in UMTS and WLAN environments in a common way also for different access technologies, by handovers and across operator domains. The basic functionality of the integrated accounting architecture proposed is also implemented as a demonstrator based on Open Diameter. This shows a proof of concept of the distributed accounting approach in terms of protocols and processes defined. The system can be extended also with other access technologies defining the required set of accounting parameters, and mapping them to Diameter AVPs.

Concluding the work, the approach presented is functional-wise complete and applicable in WLAN and UMTS inter-working scenarios, as underlying accounting management protocols of UMTS and respective ones of an IP-based network, such as Diameter, have been combined. The use of AVPs enables a flexible and extensible design, which may be enhanced to further networking technologies. Finally, the use of the Open Diameter implementation only founds a first step for a commercial system due to its developing state.

Future work in the area of distributed accounting in heterogeneous, multi-provider environments includes the design of an extended architecture, which will cover charging-specific support in terms of accounting functionality for pre-paid network access. In addition, the full integration of Diameter into cross-technology authentication and authorization mechanisms into the overall system is important. A further implementation step is to progress with the implementation to extend client and server applications, and to consider also migration scenarios defining translation agents. For a completion of a full-fledged implementation, an integration of metering functionality into the client and a performance analysis as well as tests in a real-world multi-domain environment have to be performed.

References

[1] 3GPP, *General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 5)*; TS 29.060, V5.11.0, September 2004.

[2] 3GPP, *General Packet Radio Service (GPRS); Service description; Stage 2 (Release 5)*; TS 23.060, V5.9.0, September 2004.

[3] 3GPP, *Network architecture*; TS 23.002, V5.12.0, September 2003.

[4] 3GPP, *Telecommunication management; Charging management; Charging data description for the Packet Switched (PS) domain (Release 5)*; TS 32.215, V5.7.0, September 2004.

[5] 3GPP, *Telecommunication management; Charging management; Charging principles (Release 5)*; TS 32.200, V5.7.0, June 2004.

[6] 3rd Generation Partnership Project, http://www.3gpp.org, January 2005.

[7] B. Aboba, J. Arkko, D. Harrington: *Introduction to Accounting Management*; IETF RFC 2975, October 2000.

[8] B. Aboba, M. Beadles: *The Network Access Identifier*; IETF RFC 2486, January 1999.

[9] N. Brownlee, A. Blount: *Accounting Attributes and Record Formats*; IETF RFC 2924, September 2000.

[10] N. Brownlee, C. Mills, G. Ruth: *Traffic Flow Measurement: Architecture*; IETF RFC 2722, October 1999.

[11] P. Calhoun, T. Johansson, C. E. Perkins, T. Hiller, P. J. McCann: *Diameter Mobile IPv4 Application*; Internet Draft, draft-ietf-aaa-diameter-mobileip-20.txt, August 2004.

[12] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko: *Diameter Base Protocol*; IETF RFC 3588, September 2003.

[13] P. Calhoun, G. Zorn, D. Spence, D. Mitton: *Diameter Network Access Server Application*; Internet-Draft, draft-ietf-aaa-diameter-nasreq-17.txt, Jul 2004.

[14] Daidalos EU IST Project, http://www.ist-daidalos.org, January 2005.

[15] T. Dierks, C. Allen: *The TLS Protocol Version 1.0*; IETF RFC 2246, January 1999.

[16] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry: *The COPS (Common Open Policy Service) Protocol*; IETF RFC 2748, January 2000.

[17] F. Johansson, T. Johansson: *Mobile IPv4 Extension for Carrying Network Access Identifiers*; IETF RFC 3846, June 2004.

[18] S. Kent, R. Atkinson: *Security Architecture for the Internet Protocol*; IETF RFC 2401, November 1998.

[19] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence: *Generic AAA Architecture*; IETF RFC 2903, August 2000.

[20] D. Mitton, M. St.Johns, S. Barkley, D. Nelson, B. Patil, M. Stevens, B. Wolff: *Authentication, Authorization, and Accounting: Protocol Evaluation*; IETF RFC 3127, June 2001.

[21] MobyDick EU IST Project, http://www.ist-mobydick.org, January 2005.

[22] Open Diameter; http://www.opendiameter.org, January 2005.

[23] Open Diameter Project: http://sourceforge.net/projects/diameter, January 2005.

[24] C. Rensing, H. Hasan, M. Karsten, B. Stiller: *AAA: A Survey and a Policy-based Architecture and Framework;* IEEE Network Magazine, Vol. 16, No. 6, November 2002, pp 22-27.

[25] C. Rigney: *RADIUS Accounting*; IETF RFC 2866, June 2000.

[26] C. Rigney, S. Willens, A. Rubens, W. Simpson: *Remote Authentication Dial In User Service (RADIUS)*; IETF RFC 2865, June 2000.

[27] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence: *AAA Authorization Framework*; IETF RFC 2904, August 2000.

[28] T. Zseby, S. Zander, G. Carle: *Policy-based Accounting*; IETF RFC 3334, October 2002.